

Domain: <https://demo.testfire.net> and <http://demo.testfire.net>

Vulnerability Name	Insecure cookies (Session cookies without HttpOnly and Secure flags)
Severity	4.6 - Medium
CVSS Score	Base Score: 4.6 Medium CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
Description	HTTP is a stateless protocol, which means it does not provide a mechanism for distinguishing the requests made by individual users. To overcome this issue, sessions were created and appended to all the requests. After successful authentication, cookies are set by using the “Set-Cookie” header in the HTTP response. The browser will store the cookies locally and append them to all future requests. Cookies are used mostly to achieve the below: 1. Session Management 2. Tracking To secure the cookies and reduce the attack surface surrounding the cookies, attributes were introduced which are discussed below: 1. Secure: This attribute tells the browser to only send the cookies over a secure HTTPS connection. 2. HttpOnly: This attribute prevents cookies from being accessed from the client-side JavaScript. Observation: As per the application functionality, the application can be used by a. Corporate industries b. Individual users
Impact	Misconfiguration: During the testing, we observed that the ‘Set-Cookie: JSESSIONID’ is not enabled with the 'HttpOnly & Secure' flags. If the cookie is not set with the secure flag then the client-to-server communication can be easily eavesdropped on by using the 'Wireshark' tool by performing MITM attack. If the cookie is not set with the HttpOnly flag then the cookie can be stolen in case of XSS attacks. In order to execute the MITM attack, the following conditions need to be met: a. Both the attacker and the victim users must be on the same LAN. b. Victim users have to click on the social engineering link sent by the attacker.
Vulnerable Location	https://demo.testfire.net/
Vulnerable Parameters	AltoroAccounts session cookie [missed both HttpOnly and Secure flags] JSESSIONID session cookie [missed both HttpOnly and Secure flags]
Reproduction Steps	1. Open application in the browser 2. Go to developer tools, navigate to storage and go to cookies section. 3. Check that there are no HttpOnly and Secure flags set to session cookies.
Remediation	1. Enable HttpOnly flag and Secure flag to session cookies.
Sample Code	N/A
Reference	Link1 Link2

Proof of concept:

https://demo.testfire.net/index.jsp?content=personal.htm

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Security

Other Bookmarks

Sign Off

Contact Us

Feedback

Search

Go

AltoroMutual

DEMO SITE ONLY

MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

PERSONAL

Deposit Product

Checking

Loan Products

Cards

Investments & Insurance

Other Services

Personal

Whether you're looking for a savings or checking account, credit card, or personal loan, our solutions are designed to make banking as efficient and cost effective as possible.

Deposit Products

Inspector

Console

Debugger

Network

Style Editor

Performance

Memory

Storage

Cache Storage

Cookies

Indexed DB

Local Storage

Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
AltoroAc...	ODAwMDAwfkN...	demo.testfi...	/	Session	114	false	false	None	Thu, 07 Dec 2023 1...
JSESSIO...	44547F19A3850...	demo.testfi...	/	Session	42	true	false	None	Thu, 07 Dec 2023 1...

.end